UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/321,977	05/28/1999	JOHN WANKMUELLER	AP32087-0704	7342

21003 7590 07/15/2003

BAKER & BOTTS
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER
REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
2131	3

DATE MAILED: 07/15/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/321,977	WANKMUELLER, JOHN	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-31 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-31 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement submitted is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

2. The abstract of the disclosure is objected to because on page 1, beginning at the top of the page, information from the oath and declaration is listed which is not necessary for the specification. Only the title "ASYMMETRIC ENCRYPTED PIN" and the related application information pertaining to Provisional application Serial No. 60/108,090 should remain. The information after and including "FIELD OF THE INVENTION" is okay. Where it is listed "SPECIFICATION" prior to Provisional application Serial No. 60/108,090 should be retitled "RELATED APPLICATIONS". Correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), but another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1,6,9,14-19,21,23,24,26-29, and 31 are rejected under 35 U.S.C. 102(e) as being anticipated by Ashe.

As per claims 1 and 21, it is disclosed by Ashe of encrypting (encoding) proprietary (transaction) data (col. 1, lines 37-41). A PIN is (only) encrypted (performed first encryption operation) by a master algorithm stored in memory of the smart card (col. 1, lines 45-47 & col. 2, lines 7-9). An encryption (performed second encryption operation) is performed on the propriety information (non-PIN data) by an encryption operation unique to the proprietor of the information (col. 1, lines 37-44). Ashe discloses that the proprietary information (non-PIN data) is stored in a first portion of memory and the PIN data encrypted by a master algorithm is stored in a second portion of memory which is interpreted by the examiner as cryptographically isolated (col. 1, lines 37-47 and col. 2, lines 7-9).

As per claims 6 and 24, it is disclosed by Ashe of encrypting (encoding) proprietary (transaction) data (col. 1, lines 37-41). A PIN is (only) encrypted (performed first encryption

operation) by a master algorithm stored in memory of the smart card (col. 1, lines 45-47 & col. 2, lines 7-9). An encryption (performed second encryption operation) is performed on the propriety information (non-PIN data) by an encryption operation unique to the proprietor of the information (col. 1, lines 37-44). Ashe discloses that the proprietary information (non-PIN data) is stored in a first portion of memory and the PIN data encrypted by a master algorithm is stored in a second portion of memory which is interpreted by the examiner as cryptographically isolated (col. 1, lines 37-47 and col. 2, lines 7-9). The examiner additionally interprets the teachings as including a first and second decryption operation since first and second encryption operations are performed on the respective portions of data.

As per claim 9, it is disclosed by Ashe of encrypting (encoding) proprietary (account information) data (col. 1, lines 37-41). A PIN is (only) encrypted (performed first encryption operation) by a master algorithm stored in memory of the smart card (col. 1, lines 45-47 & col. 2, lines 7-9). An encryption (performed second encryption operation) is performed on the propriety information (non-PIN data) by an encryption operation unique to the proprietor of the information (col. 1, lines 37-44). Ashe discloses that the proprietary (account) information (non-PIN data) is stored in a first portion (block) of memory and the PIN data encrypted by a master algorithm is stored in a second portion (block) of memory which is interpreted by the examiner as being analyzed to be separated from each other (col. 1, lines 37-47 and col. 2, lines 7-9).

As per claim 14, Ashe discloses of encrypting (encoding) proprietary (account information) data (col. 1, lines 37-41). A PIN is (only) encrypted (performed first encryption

operation) by a master algorithm stored in memory of the smart card (col. 1, lines 45-47 & col. 2, lines 7-9). Transactions are carried out by a user with a cash machine (col. 2, lines 13-14 & col. 3, lines 22-25) which is interpreted by the examiner as being financial information in regards to credit or debit purchases.

As per claims 15,16,26, and 27, it is disclosed by Ashe of encrypting (encoding) proprietary (transaction) data (col. 1, lines 37-41). A PIN is (only) encrypted (performed first encryption operation) by a master algorithm stored in memory of the smart card (col. 1, lines 45-47 & col. 2, lines 7-9). An encryption (performed second encryption operation) is performed on the propriety information (non-PIN data) by an encryption operation unique to the proprietor of the information (col. 1, lines 37-44). Ashe discloses that the proprietary information (non-PIN data) is stored in a first portion of memory and the PIN data encrypted by a master algorithm is stored in a second portion of memory (col. 1, lines 37-47 and col. 2, lines 7-9). The holder's (authentication requestor) PIN is later retrieved, decrypted, and verified by the microprocessor of the machine (authorized agent) and the encrypted information or proprietary information (non-PIN data) is then decrypted (col. 2, lines 50-55 & col. 3, line 32 through col. 4, line 8). It is noted by the examiner that the information on the card is transferred from the card to the machine during the verification process in order to conduct a transaction once the PIN is verified (col. 2, lines 50-55 & col. 3, line 32 through col. 4, line 8).

As per claims 16 and 27, Ashe discloses that the proprietary information (non-PIN data) is stored in a first portion of memory and the PIN data encrypted by a master algorithm is stored in

a second portion of memory which is interpreted by the examiner as cryptographically isolated (col. 1, lines 37-47 and col. 2, lines 7-9). The examiner additionally interprets the teachings as including a first and second decryption operation since first and second encryption operations are performed on the respective portions of data.

As per claims 17-19,28, and 29, the teachings of Ashe are relied upon for the use of encrypting (encoding) proprietary (transaction) data (col. 1, lines 37-41). A PIN is (only) encrypted (performed first encryption operation) by a master algorithm stored in memory of the smart card (col. 1, lines 45-47 & col. 2, lines 7-9). An encryption (performed second encryption operation) is performed on the propriety information (non-PIN data) by an encryption operation unique to the proprietor of the information (col. 1, lines 37-44). The teachings of Ashe are silent in disclosing of using symmetric and asymmetric encryption. The examiner hereby takes official notice that the use of symmetric and asymmetric encryption is notoriously well known in the art. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply both symmetric and asymmetric encryption processes as separate encryption schemes to protect different data. Symmetric encryption is notoriously well known as a system involving two transformations, one from a source and the other from the recipient which make use the either the same secret keys or private keys. Asymmetric encryption is notoriously well known as being a system involving two related transformations, one being a public key and the other being a private key whereby it is hard to determine the private key derivation from the public key derivation. The teachings of Ashe disclose of two encryption processes and it is

obvious that the use of symmetric and asymmetric encryption could have been used as separate encryption schemes whereby the choice of the particular encryption process would have been predetermined based on the benefits of the particular type of particular encryption process and the strength of the encryption which is desired.

As per claim 23, it is disclosed by Ashe of encrypting (encoding) proprietary (account information) data (col. 1, lines 37-41). A PIN is (only) encrypted (performed first encryption operation) by a master algorithm stored in memory of the smart card (col. 1, lines 45-47 & col. 2, lines 7-9). The card is placed into a slot with contactors (card reader) such as for a cash machine to read the information from the card (col. 3, lines 18-25,32-33).

As per claim 31, it is disclosed by Ashe of encrypting (encoding) proprietary (account information) data (col. 1, lines 37-41). A PIN is (only) encrypted (performed first encryption operation) by a master algorithm stored in memory of the smart card (col. 1, lines 45-47 & col. 2, lines 7-9). It is inherent that a card reader is used in the teachings of Ashe to acquire the data since it is necessary for means to read the information stored on smart card to carry out the transaction (col. 2, lines 13-14).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2,3,5,7,8,10,12,14,20,22,25, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ashe.

As per claims 2,7,10,22, and 25, the teachings of Ashe are relied upon for the use of encrypting (encoding) proprietary (transaction) data (col. 1, lines 37-41). A PIN is (only) encrypted (performed first encryption operation) by a master algorithm stored in memory of the smart card (col. 1, lines 45-47 & col. 2, lines 7-9). An encryption (performed second encryption operation) is performed on the propriety information (non-PIN data) by an encryption operation unique to the proprietor of the information (col. 1, lines 37-44). The teachings of Ashe are silent in disclosing of using symmetric and asymmetric encryption. The examiner hereby takes official notice that the use of symmetric and asymmetric encryption is notoriously well known in the art. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply both symmetric and asymmetric encryption processes as separate encryption schemes to protect different data. Symmetric encryption is notoriously well known as a system involving two transformations, one from a source and the other from the recipient which make use the either the same secret keys or private keys. Asymmetric encryption is notoriously

well known as being a system involving two related transformations, one being a public key and the other being a private key whereby it is hard to determine the private key derivation from the public key derivation. The teachings of Ashe disclose of two encryption processes and it is obvious that the use of symmetric and asymmetric encryption could have been used as separate encryption schemes whereby the choice of the particular encryption process would have been predetermined based on the benefits of the particular type of particular encryption process and the strength of the encryption which is desired.

As per claims 3 and 11, Ashe discloses of a unique (secret) key being encrypted (under a third encryption process) using a master key (col. 1, lines 45-47).

As per claims 5,8,13,20, and 30, the teachings of Ashe are relied upon for the use of encrypting (encoding) proprietary (transaction) data (col. 1, lines 37-41). A PIN is (only) encrypted (performed first encryption operation) by a master algorithm stored in memory of the smart card (col. 1, lines 45-47 & col. 2, lines 7-9). An encryption (performed second encryption operation) is performed on the propriety information (non-PIN data) by an encryption operation unique to the proprietor of the information (col. 1, lines 37-44). The teachings of Ashe are silent in disclosing of calculating a digest by applying a one-way mathematical process and to append the digest for future verification. The examiner hereby takes official notice that the use of hashing to be appended to a file and later recomputing the hash to see if the information has not be altered based on the hash values matching is notoriously well known in the art. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have used hashing

for data verification purposes. Hashing is notoriously well known as a one-way mathematical process which converts data to a specific value and when recomputing the data using the same hashing function should produce the same hash value which indicates that the data has maintained its integrity. Otherwise, if the recomputed hash values do not match with the original has value, then it is determined that the data has been altered. It is obvious that the teachings of Ashe would have benefitted from the use of hashing as a means of maintaining the integrity of the proprietary information since are directed towards a secure processing system (col. 1, lines 36-41).

7. Claims 4 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ashe in view of McKinsey.

As per claims 4 and 12, the teachings of Ashe disclose of Ashe are relied upon for the use of encrypting (encoding) proprietary (transaction) data (col. 1, lines 37-41). A PIN is (only) encrypted (performed first encryption operation) by a master algorithm stored in memory of the smart card (col. 1, lines 45-47 & col. 2, lines 7-9). An encryption (performed second encryption operation) is performed on the propriety information (non-PIN data) by an encryption operation unique to the proprietor of the information (col. 1, lines 37-44). The teachings of Ashe are silent in disclosing of an encrypted envelope which includes PIN and non-PIN data. It is disclosed by McKinsey of a Cryptolope container (encrypted envelope) which includes content (non-PIN data) and control information (PIN data) to be transferred together and the content is encrypted with a symmetric key which is encrypted with a public key (pg 2 & 3). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a

means for securely protecting data. McKinsey discloses motivation for the use of Cryptolope containers (encrypted envelopes) by reciting that it allows for both content (non-PIN data) and control information (PIN data) to be transferred together (pg 2). It is obvious that the teachings of Ashe would have benefitted from the disclosure of McKinsey as a means of transferring PIN and non-PIN together in a secure manner by means of a Cryptolope container (encrypted container) to allow for the protection of proprietary information from an illicit user.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Xiao, U.S. Patent 6,571,337

Pickett, U.S. Patent 6,012,144

Johnson et al, U.S. Patent 5,448,638

Stockel, "Securing Data and Financial Transactions"

"Programming a Distributed Application The Tuxedo System Approach"

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher Revak whose telephone number is (703) 305-1843. The examiner can normally be reached on Monday-Thursday from 6:30 am to 4:00 pm. The examiner can also be reached on alternate Fridays from 6:30 am to 3:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned as follows:

for After-Final Communications:	(703) 746-7238;
for Official Communications:	(703) 746-7239;
for Non-Official Communications:	(703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

CR
July 8, 2003